DevOps:
The Fast,
The Furious,
The Secure.

Bio

@TySbano
Sr. Director of Product Security at Target

Background
Former Application Security Director for Capital One
Former Web Application Security SME for JPMorgan Chase
Former Security Consultant for Protiviti
Semi-Active Security Geek

Education
B.S. Information Science and Technology
M.S. Information Assurance

Certifications
CISSP, SSCP, CEH, CPT

What is DevOps? Where do we put Security?

Image: Newcastleairport.au.com

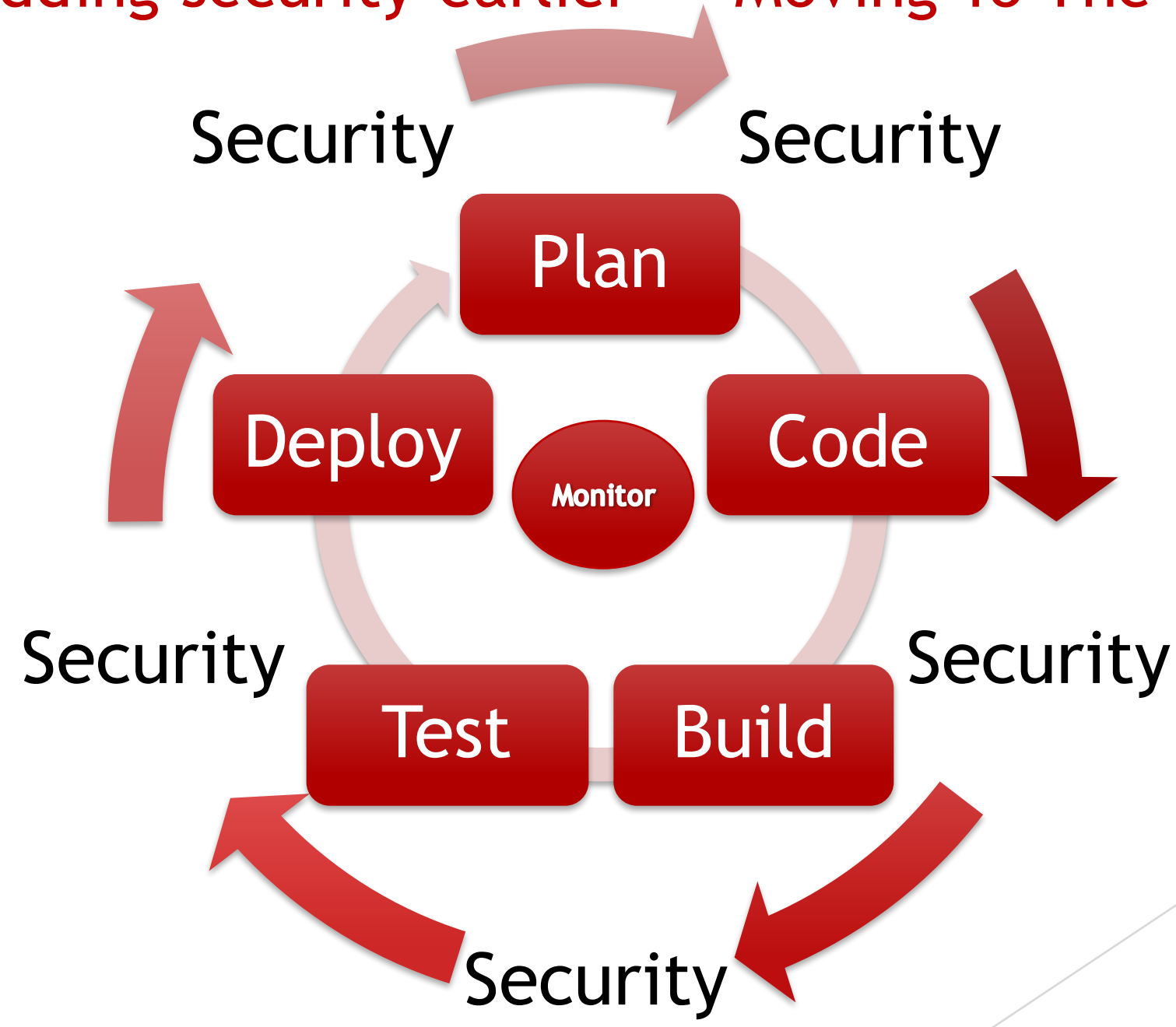
The Traditional Approach to Application Security

Gate-based Waterfall Methodology

Image: www.ajc.com

Search Engine Image Results for “DevOps Security”

Embedding security earlier – “Moving To The Left?”



Planning requires intelligent requirements

- Accessible Guidance
  - Agile Security Stories
  - Secure Coding Guidelines
  - Security Engineers
  - Technical Training

    Open Training Opportunities:
    - AppsecTutorialSeries (YouTube)
    - www.SafeCode.org

    Open Training Labs:
    - WebGoat
    - HackMeBank
    - DVWA
    - Facebook CTF?
- Threat Modeling

Test

As code is developed, security is embedded

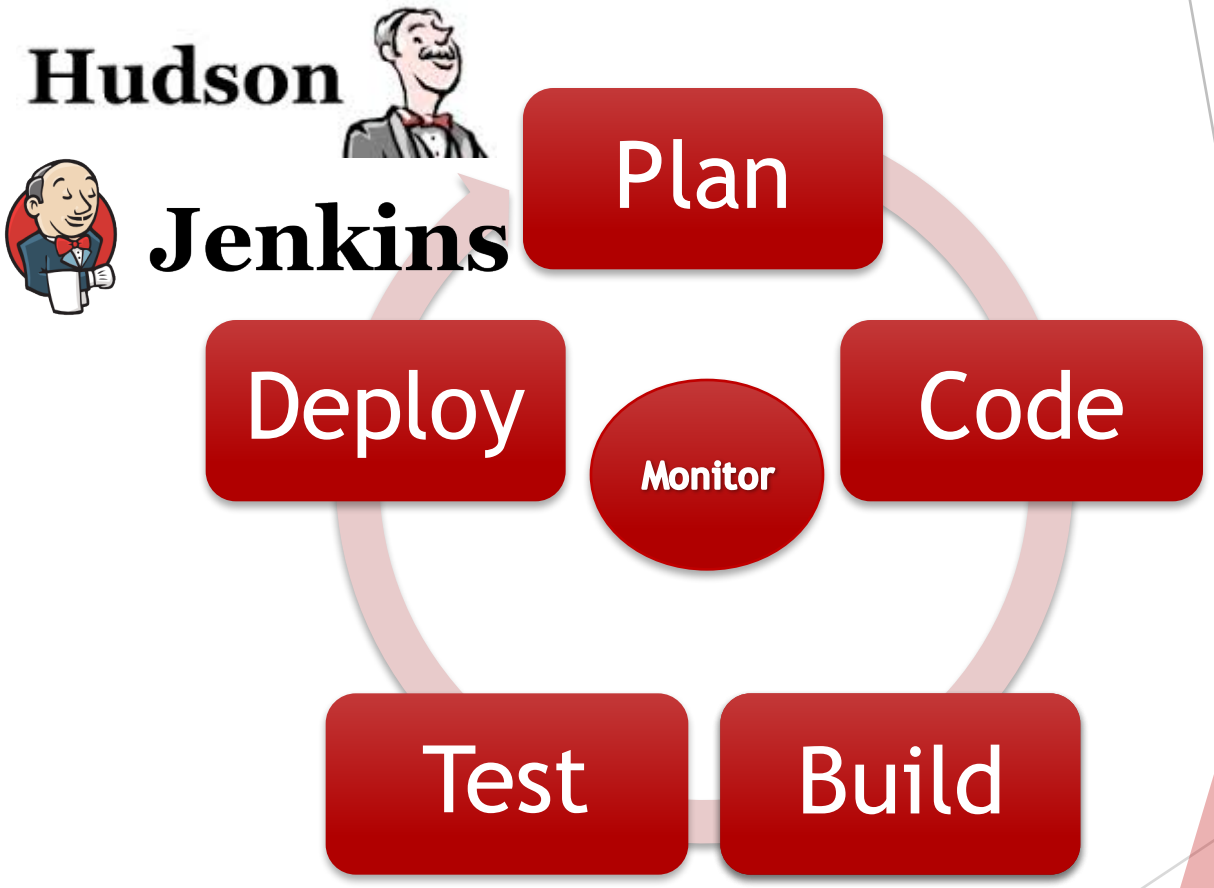
- IDE Plug-ins
  - Self-Service

- Components & Frameworks
  - OWASP Dependency Check
  - Google Search Diggity

  - ESAPI
  - .Net AntiXSS
  - Conceal

Trust & Empowerment Trumps Security Gates

- Smart Automation
  - Hudson/Jenkins
  - Controlled Scanning
    - On-demand
    - Time-based
    - Change-based
  - Static
    - Findbugs-Security
    - FxCop
    - Brakeman
    - SonarQube
  - Dynamic
    - nogotofail
    - OWASP ZAP
    - W3af / Nikto
    - OpenVAS
    - Chaos Monkey



Targeted Testing Must Be Performed By Experts

- Penetration Testing
  - Targeted Abuse Cases
  - Risk Based Testing
  - Feature Based Assessments

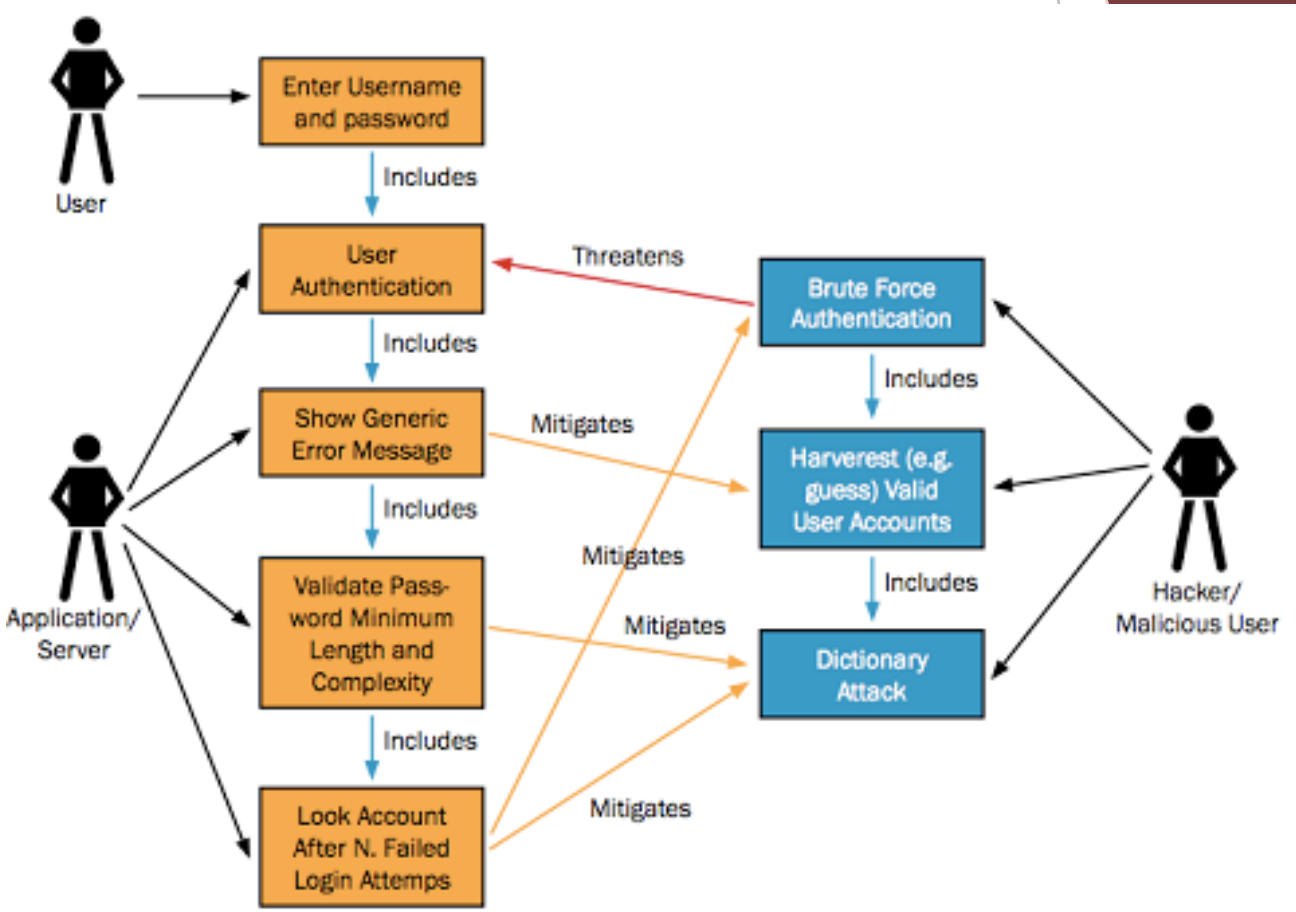


Image: www.clarotesting.com

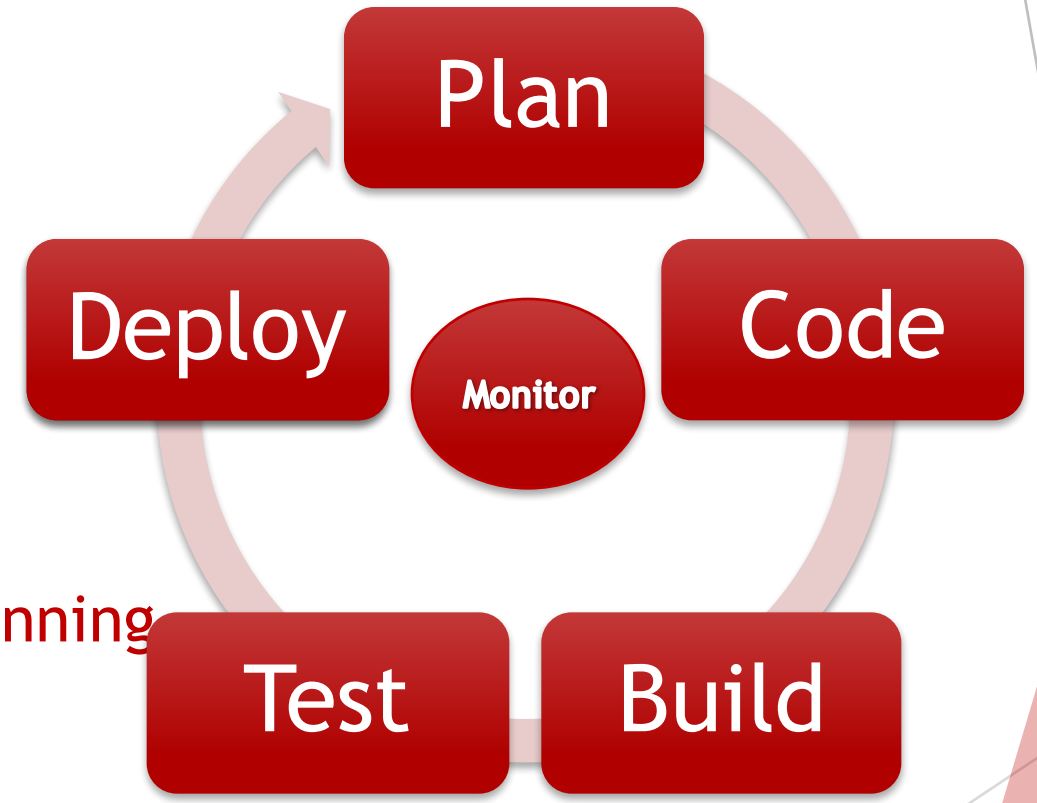
Hardened Images Enable Faster Deployment

- Build Automation

- Chef – Audit Mode

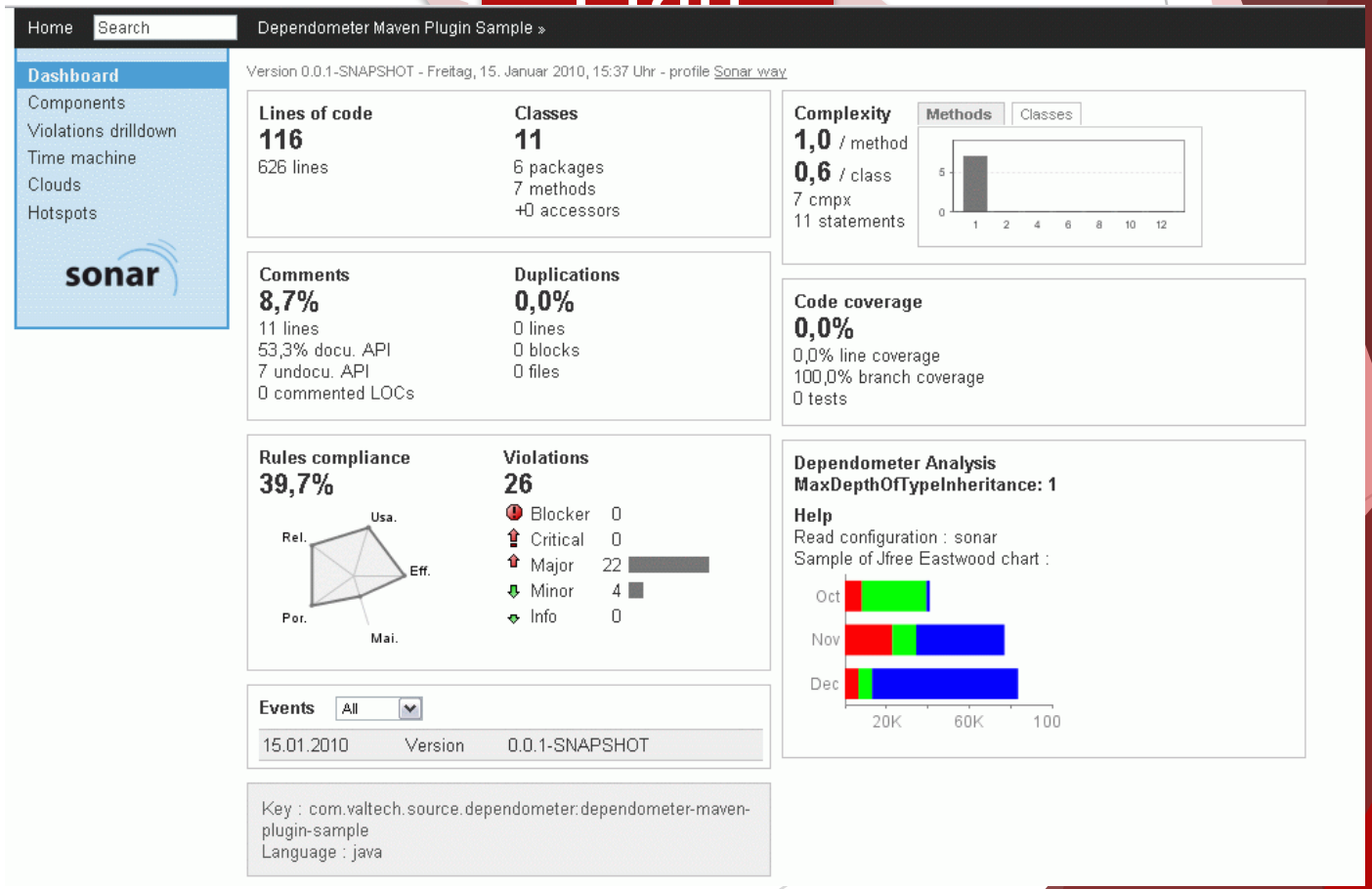
- Puppet – Security Integrity Management Platform

- Docker – Docker Security Scanning
  - …subscription service?



Continuous Monitoring, Continuous Protection

- Continuous Monitoring
  - Sonar
  - Hygieia
- API Everything!



Take-Aways

- Development Operations + Security = DevOps
- Key security practices need SMEs, but many can be automated
- Security doesn’t have to be expensive…
- Full Stack Ownership includes Security

Q & A now or later - @TySbano